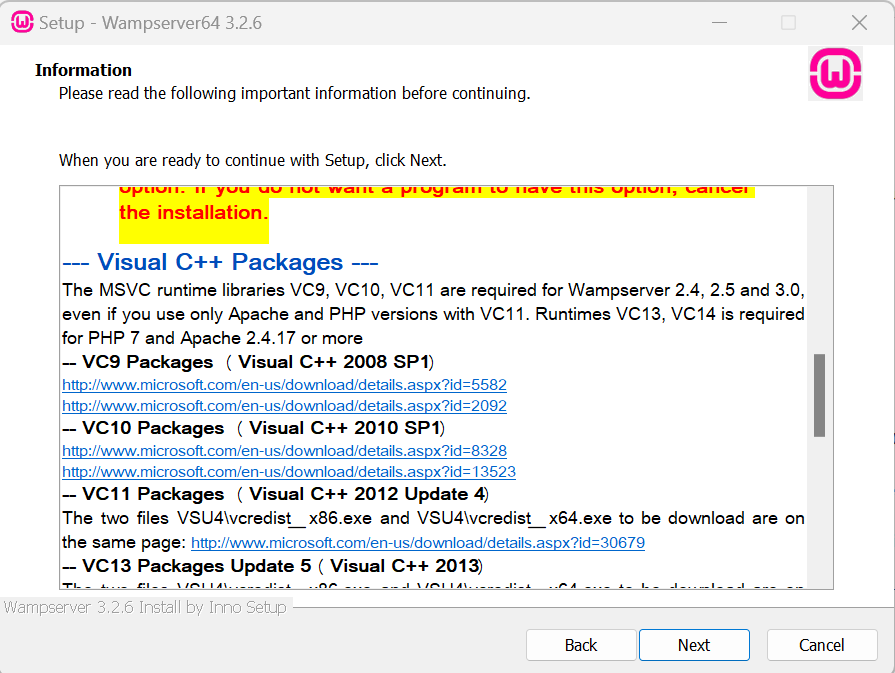
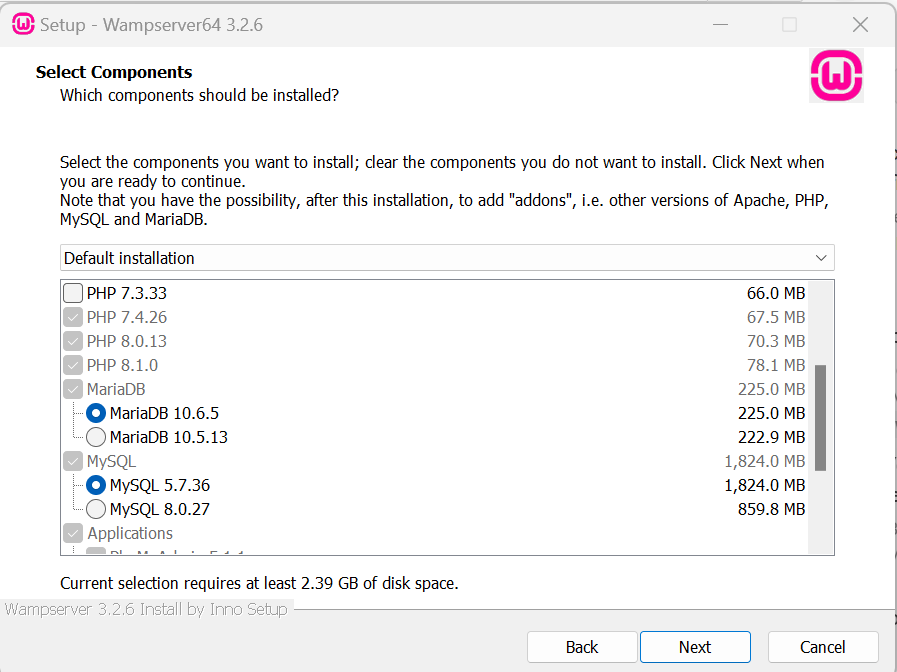
**WAMP Server**

WAMP (Windows, Apache, MySQL, PHP) Server is a virtual/local server that bundles various packages such as Windows, Apache, MySQL, and PHP into a single software for effective use. Developers/users use WAMP Server to test their websites and web applications before launching. Only Windows OS users use WAMP server and Linux users use LAMP server.

To host our website locally we installed latest version of WAMP server. For the successful installation and operation of the WAMP server different redistributable packages like Visual C++ 20012, Visual C++ 20013, and Visual C++ 20015 are also installed with it.

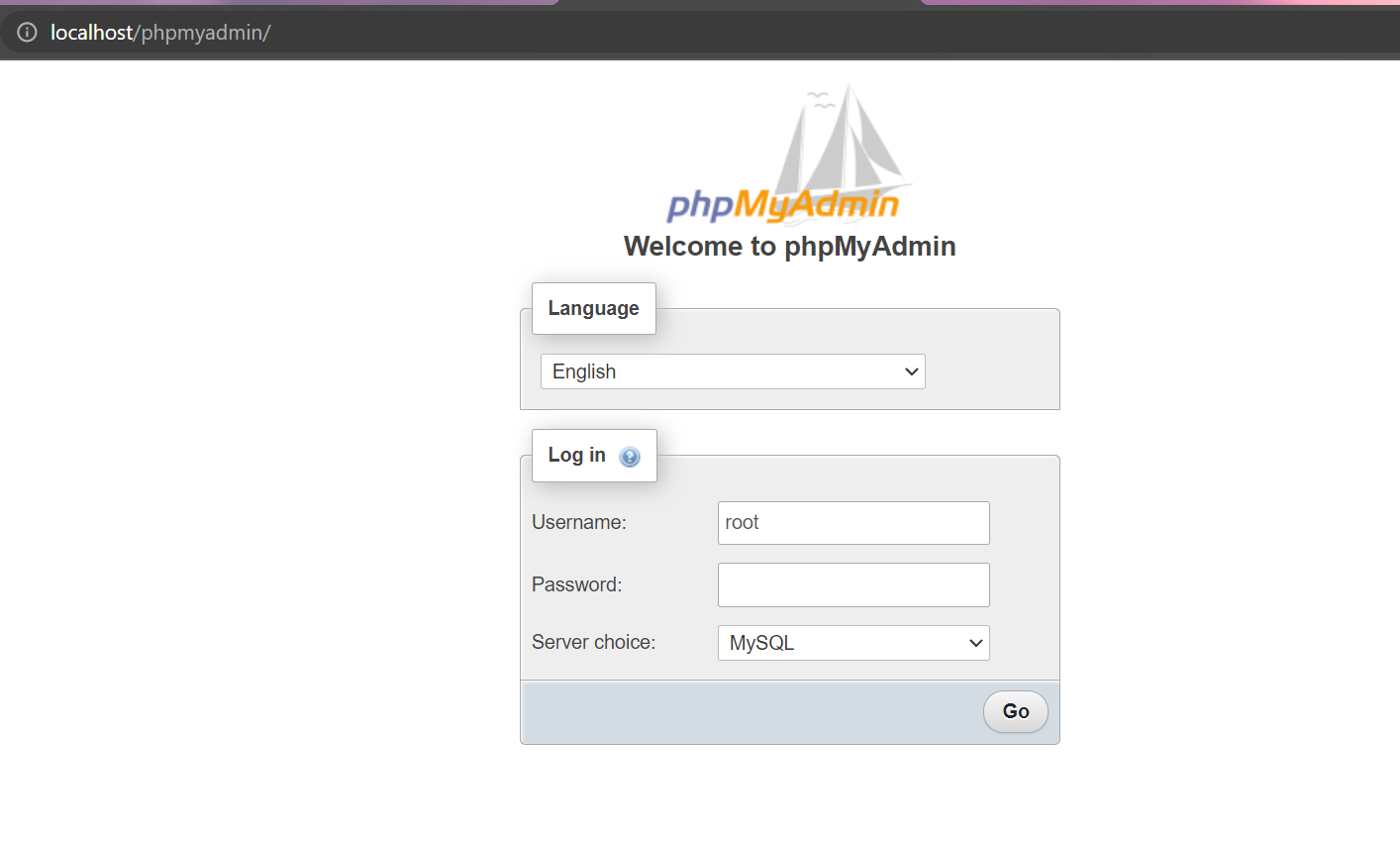


The various features that we can install when installing a WAMP server are shown in the image below. Checked features are default features that are installed by default when installing a WAMP server.

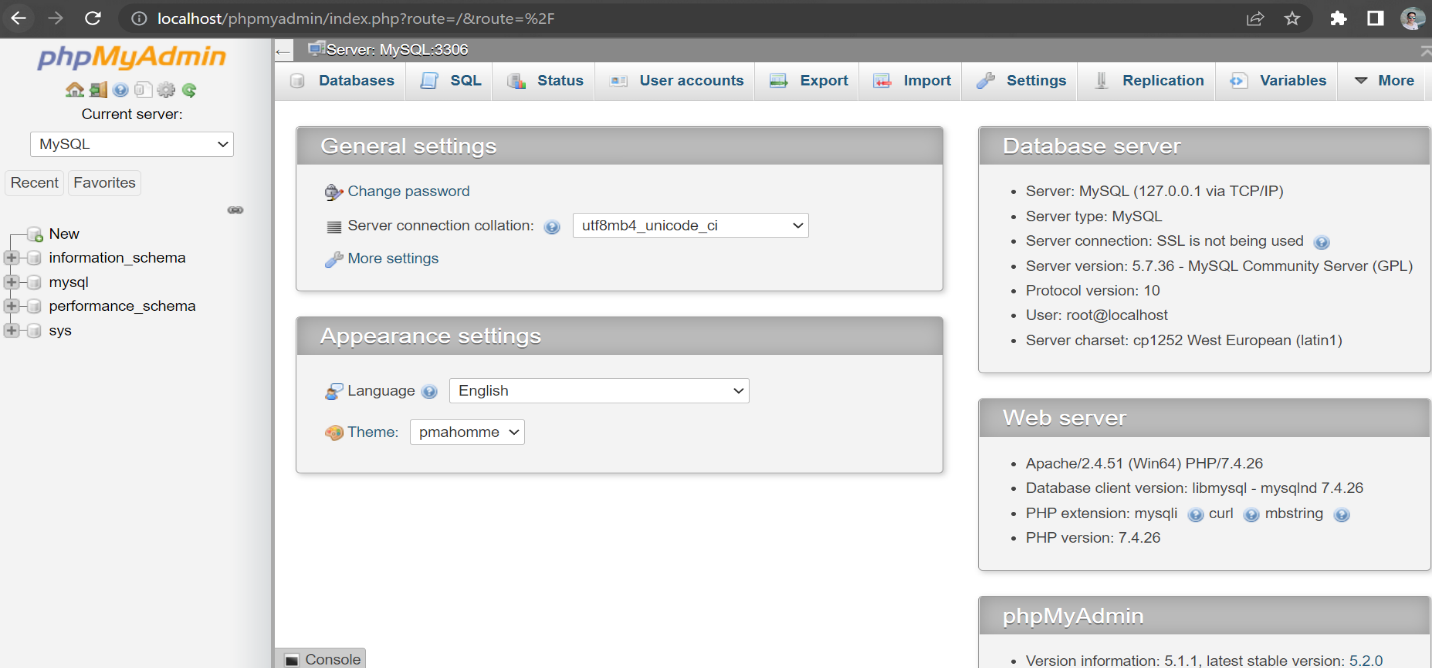


Below is an image of phpMyAdmin, which allows programmers/users to manage/create their MySQL databases using a browser. The default username and password to login to PhpMyAdmin is Username=root

Password=



Entering the default username and password opens the admin page window as shown in the image below. After entering the admin page window, developers/users can create a new database file or test their existing database file.



**Standalone vs virtual servers**

A physical server is a single user/tenant computer server, which means the physical server's resources and components are not shared/distributed among several users. Processor, memory, hard disk, network connection, and an operating system (OS) for running programs and applications are all included in each physical server due to which they are large, and costly.

A virtual server is a software form of physical server that simulates the operation of an actual physical server. On the same physical hardware multiple virtual servers can be operated. In this arrangement, a physical server's resources and components are virtualized and shared/distributed across all of the virtual serves that operate on it. A virtual server's architecture differs slightly from that of a physical server. A hypervisor is deployed on the physical hardware, such as Microsoft Hyper-V, vSphere, or VMware to run the virtual server. Virtual servers can be created and maintained using the hypervisor, each of which has its own set of virtual computing system resources.

**Physical server and Virtual server comparison**

1. **Security**

The configuration and management of security system in a virtual server is easier than that in a physical server. You have to create a protection strategy in a physical server for each server based on its computational resources, capabilities, and the sensitive data it contains. Where formerly 5 or 10 physical servers were required in your infrastructure, which can be a resource and time-consuming operation, but a single physical server could now operate 5 or 10 virtual servers. A virtual server setup, on the other hand, can be secured using a universal security method. As a result, procedures and security rules can be defined, documented, and applied via a single hypervisor interface.

1. **Management**

Physical servers are harder to maintain than virtual servers. When physical server fails, it might take many days, restoring a physical server to its former state. With the help of advanced VM backup system, recovery process for virtual server can be completed in minutes. When physical servers fails, it must be examined carefully for any flaws and, if necessary, new drivers must be installed and configured which is resource and time-consuming process. However, in the case of virtual server, physical server's resources and components are virtualized and shared /distributed across all of the virtual serves that operate on it, which are based on ready-to-use actual hardware. Virtual servers can be set up and operated in a matter of minutes, but to handle a virtual server setup is a difficult task and requires a high level of knowledge and experience.

1. **Performance**

When you deal with a lot of data that needs to be analyzed and processed in a short period of time, then physical servers are faster, more efficient and powerful than virtual servers. As a result, even having the same software and hardware capabilities and resources, a physical server and a virtual server cannot function at the equal level. A physical server is the best option if your/company's activities necessitate the most efficient use of computer resources.

1. **Scalability**

You will need more expensive software and hardware components and then go through the lengthy installation and configuration procedure to extend a physical server setup. However, a virtual server setup allows for scalability on demand without the requirement of expensive software and hardware components. Multiple virtual servers can be hosted on a single physical hardware at a time and can be changed with one click. A physical server's resources and components are virtualized and shared/distributed across all of the virtual serves that operate on it. As a result, easily configurable and manageable virtual server setups can be designed and created that can handle processes of any complexity.

**File Server Access**

A computer component where all the important data of an organization is stored and organized so that they can be accessed by other users/computers in the same network is called File server. It allows users/computers on the same network to share files and folders with each other. Only authorized users can have access to view, read, edit, delete and upload files and folders on a server. The security system of the file servers allows the admin to control weather files can be view, read, edit, delete and upload by a particular user. When the file server is configured appropriately and linked to the internet, files and folders stored on the file server can be accessed locally as well as remotely. This allows users to view, read, edit, delete and upload files and folders from anywhere on the world. File server is also used as a backup system to back up important files and folders for future use, for data recovery in case of server damage and failure, and as a repository for applications and programs needed to be available to multiple users.

This is both necessary and risky when it comes to accessing file servers by the staffs and students on-campus and off-campus. When file server is used by staff and students on-campus, there is a much lower risk of data breaches and attacks by hackers due to the file server's high security system. However, sometimes it can take a long time to complete our task and it is not possible to finish that task on-campus until it is done. So sometimes, we have to access the file server from our home or outside remotely. However, accessing the file server from outside is also risky as data can be leaked from our device, we ourselves can leak confidential data of the college, and hackers can hack our device and leak data online, which can be very problematic for our college.

**Wireless Access to Server**

Wireless access to the server allows you to connect servers from different locations within the same network (LAN).

**Practices to enable wireless access to Server**

**High-speed Internet connection**: - For wireless access to the server, you need a high speed internet connection so that your connection is not interrupted and you can access the server without any interruption and problem.

**Wireless Router**: - Routers are used to connect devices like mobile, laptops, PCs, etc. to the Internet. It acts as a gateway between the Internet and devices. A wireless router functions similarly to a wired router, except it uses wireless radio waves instead of cables to connect both within and outside the network. You need a wireless router to connect to the server wirelessly.

**Wireless network adapter: -** To connect your devices to a wireless router, a wireless network adapter is used. Wireless network adapters are pre-installed on most modern devices such as mobiles, tablets, laptops, PCs.

**Security**: - Only valid users with the correct username and password should be able to connect to the server wirelessly. This requires a firewall to be configured between the server and the wireless router, which verifies whether the user data entered by the user is valid, and only then gives the user the right to connect to the server. WPA3 (Wi-Fi Protected Access 3) security should be used for a higher level of security.

**WEP (Wired Equivalent Privacy) key configuration**: - The WEP encryption setting must be configured properly and all settings between the client and the server must be identical for WEP to work in order to access the server wirelessly.

**Issues to enable wireless access to Server**

**Connectivity to the server**: - First, check the connection between the devices and the server by pinging the server's IP address from the laptop or PC. If the server responds successfully, it means the connectivity between the devices and the router is fine. However, if ping fails, there is either a problem in configuration or break in the connectivity between devices and server due to malfunctioning of wireless router, wireless network adapter, or server.

**Slow Internet Issue**: - For wireless access to the server, you need a high speed internet connection so that your connection is not interrupted. But when the speed of the internet slows down, it interrupts the wireless connection between the devices and the server and can lead to connection loss.

**WEP (Wired Equivalent Privacy) key configuration issue**: - If the WEP encryption setting is configured improperly, you won’t be able to ping the server from wireless devices and won’t be able to access the server wirelessly.

**Remote Access to Server**

Remote access to the server allows an authorized user to connect to a server from a distance, using the internet (network connection). Remote access to the server can be set up via LAN, WAN, or even a VPN.

**Practices to enable remote access to Server**

**Enable Encryption**: - Encryption is a network security feature that secures personal, confidential and sensitive data by converting the readable data (plain text) into unreadable form (encrypted form) so that cyber criminals, hackers and other online attackers cannot access the data before it reaches its destination recipients. When the encrypted data reaches to its destination recipients, the recipients can decode the data back to its original form using their own encryption key.

**Strong password and two-factor authentication**: -To protect your system from cyber criminals, hackers and other online attackers, instead of using weak passwords you need to set strong and difficult passwords to secure your account. Use characters, special characters such as #, @, $ etc. and numbers to build a strong password and it must contain at least 8 characters. For higher level of security, two-factor authentication must be configured which provides an extra layer of protection to online user accounts. To get access to user accounts, you’ll need to pass other authentication processes such as additional user login data, biometric data, OTP authentication etc. due to which it becomes very difficult for hackers to hack your account using only your username and password.

**Use of VPN (Virtual Private Network)**: - A VPN is a security tool, which is used to protect the connection between your private network/device and public network/Internet. When you use the public network, your data is transferred over an encrypted, secure connection: the VPN server. Your data will then be routed to its final destination from the VPN server over the public network. A VPN allows you to securely access the server while simultaneously ensuring its security. A VPN is required for secure remote connection between your devices and the server.

**Issues to enable remotely access to Server**

**Slow Internet Issue**: - For remote access to the server, you need a high speed internet connection so that your connection is not interrupted. But when the speed of the internet slows down, it interrupts the remote connection between the devices and the server and can lead to connection loss.

**Insecure and Weak Passwords**: - Many users create easy and weak passwords to make it easier for them to remember passwords and such users are easy target for hackers. They also do not update their passwords regularly. This puts their data and information at risk from a variety of online attacks.

**VPN (Virtual Private Network)**: - When you remotely access the server, hackers can hack your device and leak all the files on the server. A VPN allows you to securely access the server while simultaneously ensuring its security. However, in some places, public internet services will prevent users from using VPNs. In such case, the user cannot access the server using VPN.

**Unencrypted data sharing**: - Data is the most confidential and sensitive part of all organizations. So when sharing data in unencrypted form, might cause data leakage which can be very problematic for organizations. So when users access the server remotely and share data in unencrypted form, there is a high risk of attack by hackers.

**Scalability and resilience of network system**

**Scalability of network system**

The capacity of a network to scale up or down network operations caused by sudden growth or reductions in the resources to suit increased or decreased business needs is referred to as network scalability. Scalability is one of the most important characteristics of a network.

To test the scalability of your network, the following operations should be performed:

**Data Usage**: First, determine the bandwidth usage of your network with bandwidth analysis tools. It's a metric for how much data your network resources consumed. If your network resources consume excessive bandwidth than required, it might cause variety of issues in your network and can lead to degrade the productivity of your network. In that case, you may need to upgrade your bandwidth or replace the resources that consume a lot of bandwidth.

**Number of internet connected devices**: - Determine the growth rate of internet connected devices over time and consider how many you’ll require in a year. The number and type of routers you require in your network will be determined by this.

**Hardware Resources**: - As the number of users on a network system grows, additional network hardware resources are also required to handle all the users. As hardware resources increases, it requires more physical space and consumes more power to operate all the hardware resources. If your existing location does not have required space and power to manage and operate all the additional hardware resources, you may need to expand or relocate existing space.

**Request Throughput**: - The number of requests your network resources can handle in a given time is called request throughput. This will define the maximum number of users who can access your network resources at the same time.

**Server Response Time**: - This will assist you determine how long it will take your server to respond to the request. If your server has a fast response time, it provides a better user experience as users will be able to access your services faster.

**Horizon and Vertical Scaling**

**Horizontal Scaling**

Horizontal scaling adds multiple machines/devices to your existing infrastructure to function as a single machine to meet increased demand. It is a process of increasing network capacity horizontally by adding network resources like nodes, servers etc. When network resources are added horizontally, the load balancer balances the load of the entire system by equally distributing the load.

**Vertical Scaling**

In vertical scaling, the performance of existing system is improved by adding additional computing and processing capacity. In this method, the memory, CPU, storage, and network capacity are all boosted to meet increased demand.

**Resilience of network system**

Network Resilience is the ability to operate continuously, recover quickly from failure, and the capacity to scale up or down network operations to suit increased or decreased business needs.

The different factors to make a network resilient are:

**Everything Fails**: - To make the network resilient, you need to understand that everything such as cables, routers, switches, server etc. on the network fails. To ensure the smooth operation of the network everything in the network should be maintained on a regular basis. This will allow you to keep the entire network up-to-date.

**Operating Hour**: - The second step in making the network resilient is that, a maintenance system should be created so that it maintains the entire network 24 hours a day, seven days a week, even during the operation hours of the network and ensures the proper operation of the network.

**RELIABLE REMOTE CONNECTIVITY: -** The most important thing for all organizations is a reliable and secure remote connection. For a reliable and secure connection, strong password must be used, two-factor authentication must be enabled, and VPN must be used that allows you to securely access the network resources while simultaneously ensuring its security.

**References**

* H2S Media [n.d.] What is WAMP Server and why it is used?. [online]. Available from: <https://www.how2shout.com/what-is/what-is-wampserver-and-why-it-is-used.html> [Accessed 6 Jun 2022]
* WAMP server
* Subjectmoney (2013) Gantt Chart Excel Tutorial - How to make a Basic Gantt Chart in Microsoft Excel 2013 YouTube [online]. Available from: <https://www.youtube.com/watch?v=-oD50HSBBBI> [Accessed 12 Jun 2022]
* Gantt Chart
* NAKIVO [n.d.] Physical Servers vs. Virtual Machines: Key Differences and Similarities [online]. Available from: <https://www.nakivo.com/blog/physical-servers-vs-virtual-machines-key-differences-similarities/> [Accessed 8 Jun 2022]
* Standalone vs virtual servers
* N-able [n.d.] Physical Server vs. Virtual Server [online]. Available from: <https://www.n-able.com/blog/physical-vs-virtual-server> [Accessed 8 Jun 2022]
* Standalone vs virtual servers
* Digital Guide IONOS [n.d.] File server: Definition and basics [online]. Available from: <https://www.ionos.com/digitalguide/server/know-how/file-server/> [Accessed 9 Jun 2022]
* File Server Access
* Microsoft [n.d.] Wireless Network [online]. Available from: <https://support.microsoft.com/en-us/windows/setting-up-a-wireless-network-in-windows-97914e31-3aa4-406d-cef6-f1629e2c3721> [Accessed 10 Jun 2022]
* Practices to enable wireless access to Server
* TechRepublic [n.d.] How to troubleshoot your wireless network [online]. Available from: <https://www.techrepublic.com/article/how-to-troubleshoot-your-wireless-network/> [Accessed 10 Jun 2022]
* Issues to enable wireless access to Server
* Jones IT [n.d.] Best Practices For Remote Access Security [online]. Available from: <https://www.itjones.com/blogs/2021/7/15/-best-practices-for-remote-access-security> [Accessed 10 Jun 2022]
* Practices to enable remote access to Server
* TabushGroup [n.d.] Top Challenges of Remote Access [online]. Available from: <https://www.tabush.com/blog/top-challenges-of-remote-access> [Accessed 10 Jun 2022]
* Issues to enable wireless access to Server
* Bleuwire [n.d.] Why Network Scalability Is Important for Your Company [online]. Available from: <https://bleuwire.com/why-network-scalability-important-for-company/#:~:text=Scalability%20simply%20measures%20how%20easily,up%20with%20the%20increased%20demands>. [Accessed 11 Jun 2022]
* Scalability of network system
* Suse [n.d.] Scalability [online]. Available from: <https://www.suse.com/suse-defines/definition/scalability/> [Accessed 11 Jun 2022]
* Scalability of network system
* XBASE [n.d.] How can I make my network scalable? [online] Available from: <https://www.xbase.com/2020/01/how-can-i-make-my-network-scalable/> [Accessed 11 Jun 2022]
* Scalability of network system
* TechTarget [n.d.] How to build a resilient network design [online]. Available from: <https://www.techtarget.com/searchnetworking/tip/How-to-build-a-resilient-network-design> [Accessed 11 Jun 2022]
* Resilience of network system
* Network-consultancy [n.d.] KEY ELEMENTS OF A RESILIENT NETWORK [online]. Available from: <https://network-consultancy.com/latest-news/key-elements-of-a-resilient-network/> [Accessed 11 Jun 2022]
* Resilience of network system